

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 06-274880

(43) Date of publication of application : 30.09.1994

(51) Int.Cl. G11B 7/00
G11B 7/007

(21) Application number : 05-086929 (71) Applicant : MITSUBISHI KASEI CORP

(22) Date of filing : 23.03.1993 (72) Inventor : HARAKI SUSUMU
SATO RYUHEI

(54) INFORMATION RECORDING MEDIUM AND METHOD FOR RECORDING AND REPRODUCING ITS DATA

(57) Abstract:

PURPOSE: To provide an information recording medium easily recording and reproducing data with high secrecy by recording a program incorporating an encoding command and the command decoding according to a prescribed code key on a read-only storage area.

CONSTITUTION: This medium is provided with the MO area 2 of a rewritable magneto-optical data recording area and the ROM area 1 of an optically readable read-only storage area and a hub 3 is arranged on the medium. The encoding/decoding program incorporating the command encoding the data to be written and the command decoding the encoded data read out from the area 2 is recorded on the area 1. When the program is raised the encoding of the write data and the decoding of the encoded data by a computer are performed according to the input of a prescribed encoding key. Since the data themselves are encoded and no data are utilized unless one has the code key the high secrecy is maintained. Further the program is preferred to be device driver software.

CLAIMS

[Claim(s)]

[Claim 1] Instructions which encipher data which should be provided with the Information Storage Division field which comprises rewritable data recording

regions and a read-only storage areaand should be written in said data recording regionsAn information recording mediumwherein a program including instructions which decode said enciphered data which is read from these data recording regions according to a predetermined cryptographic key is recorded on said read-only storage area.

[Claim 2]The information recording medium according to claim 1wherein said program is device driver software.

[Claim 3]In recording and reproducing systems of data in an information recording medium for a computerProvide data recording regions and a read-only storage area rewritable to the Information Storage Division fieldrecord encryption/decryption program on said read-only storage areaand by said encryption/decryption program. Recording and reproducing systems of data giving encryption instructions which encipher data which should be recorded on said data recording regionsand decryption instructions which decode data recorded by this encryption to a computer.

[Claim 4]Recording and reproducing systems of the data according to claim 3wherein said encryption/decryption program are device driver software.

[Claim 5]Recording and reproducing systems of the data according to claim 3 or 4 characterized by comprising the following.

Instructions which write data with an error correcting code in which said encryption instructions added and generated an error correcting code to said data which should be recorded in said data recording regions.

Instructions which read this data with ***** rare ***** from said data recording regionsand are enciphered according to a predetermined cryptographic key.

Instructions which overwrite data with an error correcting code written in said data recording regions with said enciphered data with an error correcting code.

[Claim 6]Recording and reproducing systems of the data according to claim 5 characterized by comprising the following.

Instructions for which said decryption instructions decode said enciphered data with an error correcting code according to a predetermined decryption keyand reproduce said data with an error correcting code.

Instructions which overwrite further said enciphered data with an error correcting code with reproduced this data with an error correcting code.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the information recording medium provided with the Information Storage Division field which comprises a read-only storage area and rewritable data recording regions in more detail for a computer and the recording and reproducing systems of the data about the recording and reproducing systems of an information recording medium and its data.

[0002]

[Description of the Prior Art] Various Information Storage Division devices are used as external storages such as a personal computer. In recent years the rewritable optical-magnetic disc equipment which mass data can record as one of such the external storages is adopted.

[0003] Generally in rewritable optical-magnetic disc equipment magnetization of the heated portion is reversed by a magnetic head and a magnetic signal is recorded at the same time it irradiates with a laser beam to the magneto-optical disc which accomplishes an information recording medium at the time of signal record and heats the magnetic recording layer locally. At the time of signal regeneration it irradiates with the weak laser beam of a grade to which a magnetic recording layer is not changed and the recorded magnetic signal is read by reading light and darkness such as the catoptric light. Optical-magnetic disc equipment has a big storage capacity which is equal to a hard disk drive and it has the advantage that media exchange is possible like the floppy disk.

[0004]

[Problem(s) to be Solved by the Invention] Since it reaches to an extreme of a magneto-optical disc like the above and it can hold a lot of data in spite of the compact outside the information of a product various [detailed] for example to important business data to can record it in the magneto-optical disc of one sheet. For this reason when an accident arises on the occasion of conveyance or mailing of a magneto-optical disc etc. there is a possibility that a lot of important information recorded on the magneto-optical disc may include a third party's hand. Also in this case in order to secure the secret about the recorded information the data recorded on the magneto-optical disc is expedient if it can restrict so that only a specific user may become accessible.

[0005] The enterprise which provides special information from an information provider slack entrepreneur for pay as one business form to the specific member who is an information user has also appeared with the rapid spread of personal computers. As information provided there is game software a music title or image software for example and personal computer communications etc. can be considered as a means to provide for example.

[0006]However if the medium which can store a lot of [that media exchange is possible and] data like ***** is used when a lot of data is provided reduction of required cost is possible when providing. In this case it is desirable if only the information corresponding to the paid fee can be restricted among a lot of information so that an information user may become accessible. That is the magneto-optical disc in which common data was stored will be prepared in large quantities information required for each of all the users can be provided if needed [the] by the thing which send each to each user and for which access to each data of the is restricted on the other hand and utility value is large especially for an information provider.

[0007]In order to respond to the request of the above-mentioned security protection or access restriction adoption of the method with which only the user who gets to know the predetermined password corresponding to the whole or a certain specific data becomes accessible to the data concerned can be considered. In this case only when this predetermined password is recorded on an information recording medium this predetermined password and the entered password are compared for example and that coincidence is detected how to make it accessible to data can be considered.

[0008]However in the data itself recorded on data recording regions since it is the usual data even if it does not know a predetermined password in the case of the user etc. who learn how to carry out physical access directly and read data for example to data recording regions it is freely accessible to data. For this reason it cannot respond to said request of the information provider about the request or access restriction of the user who needs security protection.

[0009]In order to respond to the request about the above-mentioned data access the disk driving which has a special encoder (coda) and/or decoder (decoder) is adopted. It is also thought of that only the user who uses the disk driving which has this decoder enables it to reproduce the data recorded on the information recording medium. However limiting use of an information recording medium only to specific disk driving spoils dramatically the advantage that the media exchange is possible about the information recording medium in which media exchange is possible.

[0010]Since it is performed by the function itself which an information recording medium has that this invention limits the use for the information recorded on the information recording medium only to a specific user record and reproduction of the high data of confidentiality aim at providing the recording and reproducing systems of an easy information recording medium and its data without needing use of a specific drive.

[0011]

[Means for Solving the Problem] In order to attain said purpose an information recording medium of this invention Instructions which encipher data which

should be provided with the Information Storage Division field which comprises rewritable data recording regions and a read-only storage area and should be written in said data recording regions. A program including instructions which decode said enciphered data which is read from these data recording regions according to a predetermined cryptographic key was recorded on said read-only storage area.

[0012] Recording and reproducing systems of data of an information recording medium of this invention. In recording and reproducing systems of data in an information recording medium for a computer. Provide data recording regions and a read-only storage area rewritable to the Information Storage Division field. Record encryption/decryption program on said read-only storage area and by said encryption/decryption program. Encryption instructions which encipher data which should be recorded on said data recording regions and decryption instructions which decode data recorded by this encryption are given to a computer.

[0013]

[Function] In order according to the information recording medium of this invention and the recording and reproducing systems of the data to encipher data with the function of the information recording medium itself and to record. It is easy to respond to the request of advanced security protection or the request about restriction of a data access and use of an information recording medium is not restricted only to a specific drive.

[0014]

[Example] This invention is explained with reference to Drawings. Drawing 1 is a perspective view showing the magneto-optical disc which accomplishes the information recording medium of one working example of this invention. The magneto-optical recording field (it is called MO field below) in the figure which this magneto-optical disc can rewrite [that] -- in addition it is constituted as a P-ROM (partial ROM) type magneto-optical disc of form which provided optically the read-only storage area (it is called a ROM area below) which can be read in part.

[0015] It is thin of the shape of a disk whose periphery is about 100 mm by several millimeters for example and a P-ROM type magneto-optical disc has ROM area 1 and the MO field 2 rewritable to the inner circumference side in the periphery side of a disk. The hub 3 of the MO field 2 which receives the rotation driving force from disk driving in the inner circumference side further is arranged.

[0016] The information in ROM area 1 is uniformly formed by the maker side of a disk as unevenness of the disk surface by embossing. The information in this ROM area 1 is read by the light and darkness of a laser beam in disk driving. The data in the MO field 2 is recorded by the disk driving which received

control of the computer system by the user side. The whole disk is accommodated in the jacket which accomplishes the casing which is not illustrated.

[0017]Drawing 2 illustrates typically data arrangement of each field after the beginning of using about the P-ROM type magneto-optical disc of drawing 1. In ROM area 1 sequentially from the periphery sideFor disk management. area invitation to bid12 on which the information which gives a procedureposition informationetc. for copying the information on the area 11 and a ROM area that the descriptor used was recorded to MO field was recordedthe filler 13 which accomplishes intact areaand the area 14 where initial file management information was recorded -- andThe area 15 where encryption/decryption program was recorded as device driver software is arranged. In addition to theseother information is also recordable.

[0018]The MO field 2 is a field which occupies most disks.

For examplethe field which makes a unit one sector which has the storage capacity of 600 bytes is constituted as a circumferencial direction and a field set arranged radiallyand it has the storage capacity of about about 100-600 megabytes as a wholefor example.

In the MO field 2the area 21 and 22 where the descriptor and file management information which were most copied to the inner circumference side from ROM area 1 when formatting a magneto-optical disc are recorded is arrangedand the area 23 where these are adjoined and the initialization data for codes is recorded is arranged. The area by the side of the periphery of others of the MO field 2 is the rewritable data area 24 where the data which a user actually needs is stored.

[0019]In the information recording medium of above-mentioned working exampleencryption/decryption program contains the following program partsfor example. The first program part is a program of initial setting. Since it is constituted as device driver softwareif a computer is started after a formatencryption/decryption program will rise automatically and will display a menu screen on a display first by the initialization program portion.

[0020]For this reasona user precedes actually recording data in the MO field 2and chooses code conditions suitable for the utilizing method of own information on a menu screen. In this condition selectiona data encryption first For examplean important point / that unnecessary selectionAnd selection etc. of the place which stores selection of the selection about the method of the cryptographic key for encryption/decryption for every datafor exampleis a cryptographic key set up?and whether to set one cryptographic key as the whole datathe contents of the cryptographic keyand a cryptographic key are included.

[0021]For selection of the above-mentioned initial settingthe input of a decryption key at the time of data reproduction A floppy disk (FD) the

selection about being performed by a hard disk (HD) or communication inputand being made by the manual entry of a password also being includedand needing the lock release by a cryptographic key for the degree of media use further -- or selection of a thing etc. is also included that you may cancel once. The data set up by this initial setting is recorded on other mediafor exampleFDHDetc. the area 23 of said initialization data for codes of the MO field 2and if needed.

[0022]In the case of the user who is an information providera password is set up for each [are recorded on the rewritable data area 24] data of everyrespectivelyfor example. Therebyaccording to each information user's conditionsthe information user restricts accessible data separately. In this caseto the data which performed lock release onceit sets up so that an information user may become freely accessible after that.

[0023]The second program part is a program for enciphering data. When recording data on the rewritable data area 24this program part works and enciphers the data which should be recorded by a prescribed method. For exampleon the occasion of this encryptionthe user can use that password itself as a cryptographic key by entering a different password for every data to record according to setting out in said menu screen.

[0024]The third program part is a program for the decipherment of the enciphered data. For examplewhen adopting the password itself as a cryptographic keythe same predetermined password as the time of encryption is entered as a decryption key. Processing contrary to encryption is performed to the data read by thisand it becomes decipherable by inverse transformation of the data being carried out. In this casesince data processing corresponding to the password entered when it was a decipherment will be performed if the password entered on the occasion of encryption of that data and a different password are enteredthe decipherment from the read data is impossible.

[0025]The fourth program part is a program part which performs a lock function on the occasion of encryption/decryption.

According to the conditions selected on the menu screenan enciphered program portion or a decryption program portion is controlled.

The instructions to which this fourth program part creates a cryptographic keyfor exampleIf the still more nearly same predetermined password as the time of the instructions which operate a decryption program portion according to the result of collationfor exampleencryptionis given including the instructions which compare the decryption key to which the input of a decryption key is urgedand which was ordered and inputtedIt can constitute so that the instructions of which the lock in a decryption program portion is canceled may be included.

[0026]Since it is recorded in the information recording medium of above-

mentioned working example according to a user's selection after each data is enciphered even if a third party etc. are able to access the data itself it is substantially impossible to get to know the contents. For this reason security protection very advanced about the recorded data content is possible. By having recorded encryption/decryption program on the ROM area there is also no possibility that a user may eliminate this program accidentally. This encryption/decryption program are recorded as device driver software. Since it rises automatically at the time of a startup of a computer it is only adding the input of a cryptographic key at the time of record and reproduction and the user can record and reproduce highly the data in which security protection is possible.

[0027] Next the manipulation routine of the encryption in the recording and reproducing systems of the data of the information recording medium of one working example of this invention and a decryption program portion is explained. In cipher processing in this working example encryption/decryption is performed using the error correcting code generally used at the time of record and playback of data and it is suitable for the mass information recording medium which records the information given by especially the information provider for example a magneto-optical disc.

[0028] Generally in information recording media such as a magneto-optical disc an error correcting code (ECC) is created from the data which should be recorded in order to improve the reliability of regenerative data and this is added to the data and recorded. In order especially to record 512 bytes of data for example by per one sector by a magneto-optical disc 600 bytes of data area is assigned and the method which adds and records ECC on sector portions other than 512 bytes of field where actual data is recorded is adopted.

[0029] Generally disk driving is equipped with an error correcting code generation part (ECCG) and error detection and a correction part (EDAC) for regeneration according to generation and it of above-mentioned ECC. In an error correcting code generation part ECC of a predetermined form is added to the data inputted in response to the usual light command. Data check which used the ECC in error detection and a correction part to the data with ECC read from the medium is performed. When a read-out impossible bit or an error bit exists in part the error rate of the 10^{-6} order which the medium itself has is raised for example to the error rate about a 10^{-12} order by compensating or correcting this.

[0030] With the recording and reproducing systems of the data of working example of this invention like the above it enciphers using this ECC and the situation of that encryption and decryption was typically shown in drawing 3. In the figure a computer sends 512 bytes per one sector write data A in the

main memory unit 8 to disk drivingand gives the usual light command simultaneously. In disk drivingby adding ECC to the data A of an error correcting code generation part 5 smell lever600 bytes per one sector of data B with ECC is generatedand it records on each sector of the magneto-optical disc 4 (Step S1).

[0031]Disk driving executes two kinds of commands of a form about a lead and a light command according to control of encryption/decryption programrespectively. That isif ECC will be added to write datathis will be recorded on a magnetic diskif the usual light command is given like the aboveand a light long command is giventhe data only sent from the computer will be recorded as it is. If similarly an error correction will be performed using ECCdata will be reproducedif the usual read instruction is givenand a lead long command is giventhe data currently recorded will be read as it is. Since adoption of each command form is performed by instructions of encryption/decryption programit is not necessary to adopt composition special to disk driving.

[0032]A computer gives a lead long command to disk driving according to instructions of encryption/decryption program following on Step S1. Thereby600 bytes of data B with ECC recorded on one sector of the magneto-optical disc 4 is read to the main memory unit 8 (Step S2). This data is given to the scrambler 6 next and encryption is performed by changing the arrangement of the data in the data B with ECC based on cryptographic key #1 inputted.

[0033]As the method of the encryption in the scrambler 6600 bytes of data is considered as the procession of 5x120for exampleand publicly known various compositionssuch as enciphering using the operation of this procession and the procession determined with the equation which makes a coefficient the password enteredcan be adopted.

[0034]The data C with encryption ECC of each sector obtained by encryption is given to each sector on which the original data B with ECC is recordedrespectively (Step S3)and overwrites this. About each sectors of all on which the data B with ECC was recordedthis read-out processing (Step S2) and write-in processing (Step S3) are performed one by oneand the data of each sector is rewritten by the data C with encryption ECCrespectively. For examplean information user is provided with the magnetic disk of this state from an information provider.

[0035]Even if an information user begins to read the data C with encryption ECC as it ishe cannot use this data. For this reasonit becomes [that a cryptographic key is independently provided from an information providerand this is directly inputted or given to a computer from an information provider by communication etc. by the user side etc. and] decipherable. For examplethe decryption key which corresponds about the predetermined data item to which

the fee was paid among many data items is given.

[0036]A lead long command is first given to the information user side to a drive for data reproduction. Therebydata with encryption ECC is read from the magneto-optical disc 4 for every sector (step S4)and it is given to the scrambler 6. If cryptographic key #2 is given to the scrambler 6the decipherment from the read data will be performed according to this cryptographic key #2and the original data with ECC will be reproduced on the assumption that coincidence of cryptographic key #1 and #2.

[0037]Played data with ECC B' is given to the sector on which the original data C with encryption ECC of the magneto-optical disc 4 is recorded again as it is with a light long command (Step S5)and the data C with encryption ECC is overwritten by this data B'. This rewriting is performed for every sector. After all the sectors are overwrittenby the usual read instructiondata with ECC B' is read (Step S6)it is given to error detection and the correction part 7and the same regenerative data A' as write data A is obtained.

[0038]In the recording and reproducing systems of the data of above-mentioned working exampleonce decryption is performed by the user sidethe data C with encryption ECC on a magnetic disk will be rewritten by usual data with ECC B'and the use of data of it will be attained only with the usual read/write command after that at **. For this reasonthe input of a decryption key for the second time is unnecessaryand rewriting of subsequent data is forbiddenfor example by initial setting.

[0039]In the case of the user aiming at the usual security protectionWhenever it replaces with above and reproduction of each data is completedthe composition which prevents surreptitious use of the data by a third party is also employable by always enciphering and recording data by repeating Step S1 - Step S3 following on Step S6.

[0040]Although above-mentioned working example showed the example which performs this encryption/decryption for every sector on the occasion of encryption/decryptionand rewrites former data each timetaking into consideration the capacity of the main memory unit in not the thing to restrict to this but a computer -- two or more sectors at once -- or it is also rewritable by enciphering / deciphering one data.

[0041]In the case of initial settingit replaces with the usual input and collation system of a passwordand a part of encryption / decryption program are cut offor exampleit records on other recording media as an external programand this external program can also be considered as substitution of a cryptographic key. In this casethe composition which starts this external program itselffor example by the input of a password is also employable.

[0042]When adopting the composition which stores the password for collation in other recording mediafor exampleFDHDetc. or when adopting the recording and

reproducing systems of the data of said working example which does not need the collation of a password itself it is impossible to rob the information recording medium itself of these passwords. Therefore it becomes impossible substantially for an illegal use person etc. to decode the data which was enciphered by the information recording medium and recorded on it and the security protection very advanced about the recorded data of it becomes possible.

[0043]

[Effect of the Invention] As explained above according to the information recording medium of this invention and the recording and reproducing systems of the data. The record and reproduction of high data of confidentiality are attained without performing the encryption and decryption of data which should be recorded with the function of an information recording medium and not needing use of a specific drive and being accompanied by a user's burden.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The perspective view showing the structure of the P-ROM type magneto-optical disc which accomplishes the information recording medium of one working example of this invention.

[Drawing 2] The block diagram which illustrates typically arrangement of the data in the magneto-optical disc of working example of drawing 1.

[Drawing 3] The block diagram showing typically the situation of record and reproduction of the data of an information recording medium based on the recording and reproducing systems of the data of one working example of this invention.

[Description of Notations]

- 1: ROM (read-only memory) field
- 14: Initial file management information area
- 15: Encryption/decryption program area
- 2: MO (magneto-optical recording) field
- 22: File-management-information area
- 23: The initial-setting data area for codes
- 24: Rewritable data file area
- 4: Magneto-optical disc
- 5: Error correcting code generation part (ECCG)
- 6: Scrambler
- 7: Error detection and a correction part (EADC)

8: Main memory unit
